Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 29 (2012) 3583 – 3588

Procedia Engineering

www.elsevier.com/locate/procedia

2012 International Workshop on Information and Electronics Engineering (IWIEE)

Research on the SCADA System Constructing Methodology Based on SOA

Liang Wang*, Xiuting Wang

School of Computer Science and Technology,Harbin institute of Technology(weihai),Weihai ,264209,China

Abstract

With the rapid development of information technology, People become more and more dependent on the automatic technology in some special industries like oil, electricity and chemistry. As a novel technology, SCADA is widely deployed in these field, which greatly reduce the manpower requirement and improve the efficiency at the same time. Yet the data patterns produced from different RTU(Remote Terminal Unit)s are not compatible, which bring some difficulties for the secondary development of software for data collecting and analyzing. Regarding this problem, SOA is introduced to the constructing of SCADA and a novel methodology is proposed. The workflow of the methodology is described in detail. A case for SCADA constructing in electricity industry is given, which prove the validity of the method provided.

Keywords: Supervisory Control And Data Acquisition; Service oriented architecture; Enterprise Service Bus(ESB)

1. Introduction

SCADA[1] (Supervisory Control and Data Acquisition) is a system to automate industrial control and monitoring. SCADA includes field sensors, Programmable Logic Controllers (PLC) and Remote Telemetering Units (RTU). SCADA use can be found in power generation, manufacturing automation, oil and gas exploration and utilities monitoring and control. SCADA can be used to monitor parameters such as temperature, pressure, flow rate, pH, etc. SCADA can set off alarms based on collected and observed data and remote access function can be enabled through a web based interface or specialized software on networked machines. With the advantage of high efficiency and excellent environment adaptability,

* Corresponding author. Tel.: +86-0531-8277-6569;.
E-mail address: wangliang123@gmail.com.

doi:10.1016/j.proeng.2012.01.535

SCADA is widely employed in a lot of industry fields. Although the SCADA is widely, there are still some shortcomings like data fusion and data mining on the data acquired from RTU. Regarding this problems, the Service-oriented architecture is introduced and a system constructing method is proposed which will improve the efficiency and reduce the labor cost. The case of electricity using ESB is employed to prove the validity of the method proposed.

2. Related works

With the significant advantages, the research on the data fusion and secondary developing based on the data acquired attracts a lot of scholars in not only academy but also industry. Some achievements have been made in this field, some reprehensive ones can be listed as follows. Igure, Vinay M.[2-4] provides an overview of all the crucial research issues that are involved in strengthening the cyber security of SCADA networks, describes the general architecture of SCADA networks and the properties of some of the commonly used SCADA communication protocols and the ongoing work in several SCADA security areas such as improving access control, firewalls and intrusion detection systems, SCADA protocol analyses, cryptography and key management, device and operating system security, concludes with an overview of these standardization efforts. Kilpatrick, Tim[5-7] describes an architecture for SCADA network forensics. In addition to supporting forensic investigations of SCADA network incidents, the architecture incorporates mechanisms for monitoring process behavior, analyzing trends and optimizing plant performance. Kang, Dong-Joo analyzes the SCADA network vulnerabilities on the aspects of cyber security. Robles, Rosslin John[8-10] discuss internet SCADA, which is connected through wireless communication and the security issues surrounding it and a symmetric-key encryption for wireless internet SCADA is proposed. These achievements mainly focus on the reliability and security of SCADA networks, few of them researches on the format translating between data from different RTUs. To well fuse the data acquired, and provide rich support for the upper application, ESB, a classical SOA technology is introduced, and the result is validated with the case provided.

3. Construction of SCADA System

Because of noise in the course measure, data from optical triangular scanners is preprocessed, which includes smoothing, removal noise and deleting exceptional points, before reconstructing surface is cable of identification clouds and process, the minimum distance is found automatically and tandem compound to acquire point group. Cut point group along a certain direction to obtain cross-section these are continuous and in a sequence [4].

3.1. Summary of SOA

SOA is an architectural model, which can be used to make distributed deployment, composing and application for loosely coupled coarse-grained application components according to the requirement. All of the functions or services of SOA can be defined using the description language, and their interfaces defined using an independent, free service implementation where the hardware platform, operating system and programming language effects.

The SOA holds two features as follows. (1) Standardization of data formats. It can be encrypted and compressed data format to improve the safety and real-time, the different data formats into a unified standard format, such as XML format. (2) Unified standard interface. It can be a variety of interfaces into a unified standard interface. There are variety of SOA products, and the most popular one is ESB(Enterprise Service Bus). This paper will apply ESB to the data processing of SCADA.

ESB is a traditional middleware technology and XML, web services and other technologies of the product. ESB is a services and applications in loosely coupled integration between the standard way. ESB functions can be simply summarized as these aspects: the routing of messages between services and service; in the transition between the requester and service provider transport protocol; in the conversion between the requester and the service message formats; processing from the kinds of heterogeneous sources of business events; ensure service quality and safety, reliable and interactive processing.

3.2. SCADA system data fusion process

To construct the SCADA system for providing better support to the data fusion and data analyzing. The structure of SCADA system should be constructed accordingly. The D-S evidence theory should be employed for the SCADA data fusion, the process can be described like figure1.

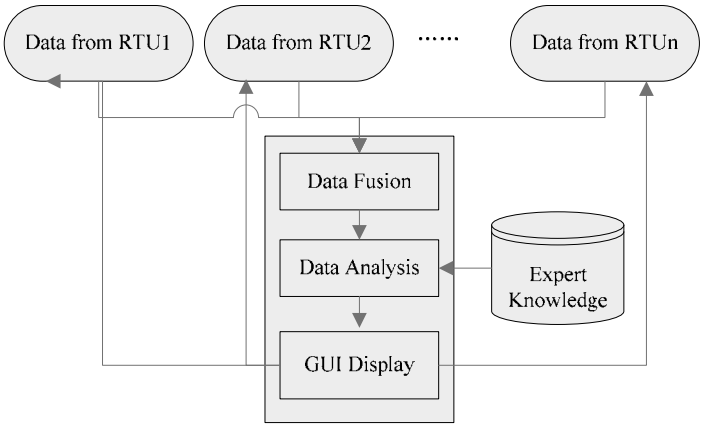

Fig. 1. *the data fusion process of data from different SCADA*

D-S Evidence is a statistical-based data fusion classification algorithm, is used when the information sources contributing information cannot associate a full probability of certainty to their output decisions. D-S evidence theory applies belief function as measurement, which allows one to quantify the confidence that a particular event could be the one observed. Then, while new information arrives, the identification system integrates it using conditioning rules to provide a representation of the obviousness of the situation. The process of SCADA data fusion can be described as follows.

Algorithm 1:SCADA data fusion

- Begin
- Calculating basic probability assignment function m , belief function Bel and likelihood function Pal of various data sources according to formula

$$Bel(\{A\}) = \sum_{B\subseteq\{A\}} m(B) \tag{1}$$

- Initializing the belief function

$$Bel(H) = \sum_{B \subseteq H} m(B), Bel(\phi) = 0, Bel(\Theta) = 1 \tag{2}$$

- Under the combined effect of all the evidence calculation of the basic probability assignment function according to the evidence fusion rule

$$m_{12}(H) = m_1(H) \oplus m_2(H) = \frac{\sum_{B \cap C = H} m_1(B) m_2(C)}{\sum_{B \cap C \neq \phi} m_1(B) m_2(C)} \tag{3}$$

- Choose to support the hypothesis that of the greatest possibility according to the decision making rule.
- Output the Result of Data Fusion
- End

3.3. SCADA ESB constructing method

To employing the Data fusion algorithm mentioned in 3.2. The SOA should be designed to make a connection between RTUs and upper application. The detail of SOA can be divided into three steps.

(1)Top level structure constructing. In this step, all the data patterns of RTUs should be gathered for the development of ESB. Generally speaking, the structure can be divided into three parts, including Kernel service layer, which provides a bus service and data exchange platform, the system messaging between software modules, standard data format conversion, service authentication, security management, application layer, which Includes the entire top of ESB-based application development and system integration, system will come with ESB standards and formats and interface managing layer, which complete communication with the bottom of the device based on a variety of interfaces, data formats standardized processing, communication with a variety of subsystems.

(2)Communicating layer design. This step includes two sub-steps, including From the remote terminal to the dispatch center of the upstream information transfer process, From the dispatch center to the remote terminal's downlink information transfer process. Remote information collection will focus on the collection to the local direction of the distributed collection, mainly for remote serial communications and Ethernet communication mode in two ways. Serial communication, the communication is point to point, while the use of Ethernet, the communication is a multipoint, with the master station can simultaneously exchange data with each remote terminal unit, RTU is necessary to establish multiple channels, each channel different application-layer communication protocol. Complete front-end communications equipment based communication with the lower end, a variety of interfaces, data formats standardized processing, communication with various subsystems to complete the format conversion, to the requirements of ESB, ESB became the basis for tools.

(3)Network topology design. In this step, Remote information collection will focus on the collection to the local direction of the distributed collection, mainly for remote serial communications and Ethernet communication mode in two ways.

(4)Letter-layer software architecture design. In this step, explain some of the Statute and Communication and interface part of the ESB are included.

(5)Programming environment and database. In this step, C + + language to be used for program development system on Windows NT, Microsoft SQL Server provides a strong support of the data in the

database to provide effective management and use of effective measures to achieve data integrity and data security case.

4. Case Study

To prove the validity of the method described, the process of electricity system constructing process using ESB is described.

Top level structure constructing. This step will construct the global design of the electricity SCADA system with ESB, which can be described like figure 2.

The steps followed can be executed like the method mentioned in 3.3. through this case some achievements can be reached. The current SUB station communications and ESB communication protocol used in more types, RTU from different manufacturers, and each RTU to the dispatch center sending the data, the use of the statute are not the same, there is also the same understanding of the Statute of different manufacturers deviation, resulting in inconsistent communication protocol implementation, access control center, the workload is relatively large. Remote communication protocol, including circulating remote protocols and response style of the Statute.

In the SOA platform for electricity SCADA system design, its nuclear Heart is the overall system architecture based on SOA design. In this paper, Study the overall system architecture based on SOA design of the communication layer Architecture design, the use of mature middleware products currently include international Enterprise Service Bus (ESB), messaging middleware to open a second Hair, get the following conclusions.

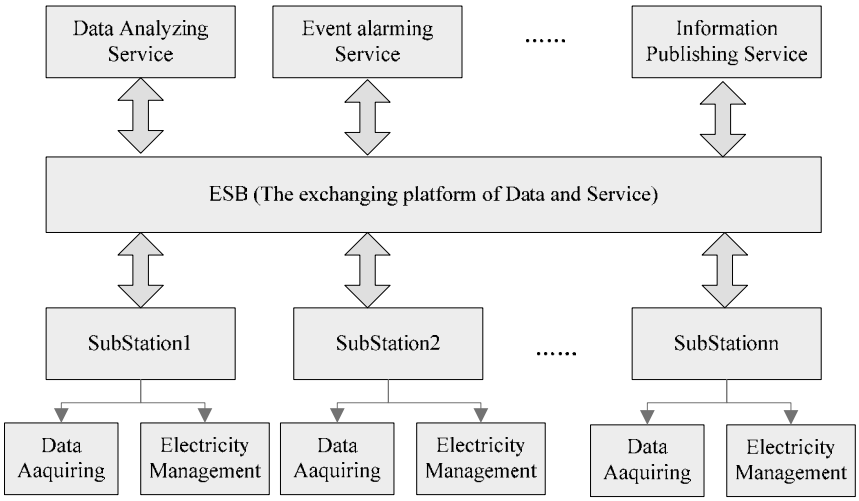

Fig. 2. the global design of electricity SCADA system

(1) SOA is a service we offer data exchange with the total Line platform, the system messaging between software modules, standard data format conversion, service authentication, security management.

(2) standard interface, a standard data format to reduce the off The ability to send personnel requirements and language restrictions.

(3) can greatly improve the front-end and back-office data transfer Rate and real-time communications.

5. Conclusion and Future Works

As SCADA network are more and more popular for the industry application , the data fusion and analyzing problem become more and more prominent. Traditional method paid much attention on the reliability and security of SCADA network, yet some factors like convenience and usability are neglected. This paper introduced the concept of SOA and described ESB a classical SOA application, then the ESB is used for constructing the SCADA network and data analyzing, the detail process with D-S evidence theory is talked exactly. The case of electricity is provided to validate the validity of the method provided.

References

[1].Dodds, D., SCADA system replaces aging, proprietary DCS. *Control (Chicago, Ill)*, 2005. 18(4): p. 60-62.

[2].Igure, V.M., S.A. Laughter, and R.D. Williams, Security issues in SCADA networks. *Computers and Security*, 2006. 25(7): p. 498-506.

[3].Linder, G. The importance of standard SCADA protocols to the reliable operation of distributed farm-scale anaerobic digesters. 2009. Seattle, WA, United states: *IEEE Computer Society*.

[4].Sanchez, J., Municipality upgrades to wireless SCADA system for future growth. *World Pumps*, 2006(474): p. 30-33.

[5].Kilpatrick, T., et al. An architecture for SCADA network forensics. 2006. 233 Springer Street, New York, 10013-1578, United States: *Springer New York.*

[6].You, J.-X., et al., Sate estimation using SCADA and PMU mixed measurements. *Gaodianya Jishu/High Voltage Engineering*, 2009. 35(7): p. 1765-1769.

[7].Xia, S., et al., Dual-server undisturbed switching algorithm for the substation SCADA system. Dianli Xitong Zidonghua/*Automation of Electric Power Systems*, 2006. 30(14): p. 58-61.

[8].Robles, R.J. and M.-K. Choi. Symmetric-key encryption for wireless internet SCADA. 2009. Tiergartenstrasse 17, Heidelberg, D-69121, Germany: *Springer Verlag.*

[9].Stoian, I., et al. SCADA on hydro power plant cascade - Case study. 2007. Cluj-Napoca, Romania: *IFAC Secretariat.*

[10].Nguyen, V.I., W. Benjapolakul, and K. Visavateeranon. A high-speed, low-cost and secure implementation based on embedded ethernet and internet for SCADA systems. 2007. Takamatsu, Japan: *Society of Instrument and Control Engineers*